Communicator

Articles

EQUIVUS

How Secure Is Your Customer Data?

"According to Forrester Research, the global economic damages caused by security breaches totals more than $15 billion each year."

It is hard to resist the benefits of wireless data connectivity to PCs, personal digital assistants, virtual private networks, work at home access and cellphones.

Mobility, collaborative commerce and work at home initiatives are redefining the security boundaries of the "virtual enterprise." Enterprises must take increasing care to secure internal, external, wired and wireless communications.

An enterprise's network security planning and precautions may be excellent within the anticipated areas of vulnerability. However, the enterprise's security efforts will be fruitless if this planning was based on false assumptions about who can access the network, how they might do so, and what value they may place on the information available.

Let's review the three most common false assumptions about remote-access security, discuss the dangers of each and offer recommendations to protect against them.

Assumption #1 – We Don't Have Any Unauthorized Remote Access

Setting up unauthorized dialup remote access is easy for users and hard for IT managers to discover. With emerging Web remote-control tools, the problem is migrating from dial up to Internet access and growing in proportion.

Recommendation

Scan phone lines using commercial "war dialers". This will detect and eliminate unauthorized dial-up connections.

Assumption #2 – We Have Control of Our Wireless LANs

Many enterprises mistakenly believe that all of the access points used for wireless networking in their organizations are under their control. Recently, however enterprises have discovered "rogue" wireless LAN access points that clever users had setup in the buildings. Corporate intranets were publicly exposed – in locations with public access and collocated with competitors.

Today any user can purchase a wireless LAN access point at prices that have fallen to less than $150.

Recommendation

Enterprises must monitor wireless LAN activity to ensure that unauthorized access points are discovered and removed quickly.

Assumption #3 – We Don't Have To Worry Because Our Information Isn't Worth Stealing

Enterprises that believe this assumption expend less effort and vigilance on security, and the effect trickles through their operations, resulting in weak security practices. Hackers are not simply thieves. They are looking to exploit networks. They can enter an enterprise's network and stage an attack against a third party. Who needs that publicity?

Recommendation

Recognize that no enterprise information should be immune from scrutiny to secure and protect it, and that network security is everyone's business. No one in the enterprise is too unimportant to follow security best practices.

Protect Your Business From Disaster

What's Your Plan?

In the aftermath of recent natural disasters, terrorism, service provider failures, internal and external sabotage, computer virus attacks and equipment breakdowns, businesses have recognized more than ever the need for an organization to be prepared. Companies are striving to meet the demand for continuous service. With the growth of e-commerce and other factors driving system availability expectations toward 24x365, the average organization's requirement for recovery time from a major system outage now ranges between 2 and 24 hours. A requirement driven by the expectation an organization faces on all sides.

Business continuity planning and disaster recovery planning are vital activities. However, the creation of (and maintenance of) a sound business continuity and disaster recovery plan is a complex undertaking, involving a three-step process. The result is a set of plans for all four areas of business continuity: disaster recovery, business resumption, business recovery and contingency.

Step 1: Establish the Foundation – The first step in a sensible business continuity process is to consider the potential impacts of each type of disaster or event. This is critical – how can you properly plan for a disaster if you have little idea of the likely impacts on your business of the different scenarios? After determining the business impacts, it is now equally important to consider the magnitude of the resulting risks. Again, this is a critical activity – it will determine which scenarios are most likely to occur and which should attract most attention during the planning process.

"Two out of five enterprises that experience a disaster - go out of business within five years. Business continuity plans and disaster recovery services ensure continuing viability." Gartner Group

Step 2: Develop and Implement the Plan – A sound disaster recovery and business continuity plan is essential to protect the well being of an organization. Yet, many enterprises still side step the issue or hold plans that are clearly out of date or inadequate. Part of the reason for this is the complexity of the task. Initiating a company's first integrated business continuity plan and managing it can be overwhelming. More importantly, the effort is sometimes beyond the expertise of the company's internal team charged with developing the plan. Often, even if internal team members are up to the task, the company cannot afford to take them away from their primary corporate responsibilities. The best first decision may well be to select an experienced consultant to assist at least the start-up project. Such an advisor can provide insight into later decisions about which processes to maintain internally and which to outsource.

Step 3: Maintain the Plan – Once the recovery/continuity plan has been created, it is important to ensure that it remains up to date and workable. Decades of industry experience have proven that business continuity planning that lies forgotten in a desk drawer is of little practical use in a real emergency. Organizational and staffing changes alone dictate the need for frequent testing, updating, auditing, training and communications.

Keys to success – Business continuity planning, strategy, implementation, and maintenance must take into account all aspects of business continuity- data, finance, buildings, communications, equipment, personnel, customer service, knowledge assets, etc. Executive management involvement and support across all units of the organization is critical.

Insulate Your Business From Telecom Turbulences

MCI WorldCom, Adelphia, Qwest,…the list of telecom providers declaring bankruptcy or teetering on the edge continues to grow. Are you relying on one of these service providers for your telecom and data network needs?

The turbulence throughout telecom has left enterprises vulnerable to the day-to-day fate of their providers. The loss of telecom and data network services, even for a short outage, means unhappy customers and substantial loss in revenue.

Businesses are caught between two unattractive alternatives:

➢ Do nothing and hope for the best

➢ Switch providers at considerable expense, with no guarantees

There is a third alternative that will quickly insulate your business from telecom turbulence, without impacting your existing telecom and data networks. This alternative is a Telecom and Data Network Business Protection Program.

The keys to the program:

➢ Identify immediate contingency for your most vulnerable applications and sites

➢ Identify cost effective options for both corporate and remote sites

➢ Minimize impact on your existing telecom and data network (minimize internal team member support time involved in changing networks)

➢ Augment existing carrier contracts (just because a vendor files bankruptcy, does not mean your contract is null and void)

There are solutions available today that require no new operations resources, no proprietary hardware, little or no capital outlay, allow temporary or permanent solutions and offer quick service install within 24 hours.

Creating your company's personalized Telecom and Data Network Business Protection Program today will insulate your business from unexpected telecom and data network service interruptions. ■

Success Story

CPA Firm Reduces Fax Expenses By Thousands Per Month

Background
A CPA firm was using an Internet fax service provider to receive and send faxes electronically. A change in the pricing policy by the service provider sent fax charges skyrocketing.

Challenge
Identifying a more economical solution became a necessity. The CPA firm did not want to return to multiple fax machines and paper output. They required a system with electronic distribution and storage of the incoming faxes.

Solution
The firm contacted Equivus Inc. to identify the market options.

Equivus followed their four-step solution delivery process to identify business requirements and current technological capabilities. Equivus identified a server based fax solution meeting all business requirements and integrating with the current technology base. The solution installation and staff training were complete within a week. The solution provides the CPA firm control over inbound and outbound fax capabilities, electronic storage and distribution of files.

Results
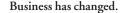The solution yields operating cost savings of thousands a month. ■

About Equivus

The world has changed. The clear line between business strategy and technology strategy is gone. So is the notion that technology implementation follows leisurely behind strategy.

Business has changed. The best businesses in the world today treat technology advantage as an ongoing business strategy. They expect to execute, upgrade and innovate continually.

Who do you need? You need great people. People who can move easily between concepts of technology and of business. Like the strategic consultants at Equivus who provide concrete business models, focused strategies and real-life solutions for companies in dozen of industries, including yours.

Who we are? Equivus is a full-service consulting practice - with seasoned business and technology consultants. Our consultants are expert in business, technology and marketing strategy, organizational change and design. With a deep understanding of both technology and business strategy, we help position companies for today's fast-changing economy.

Equivus consultants specialize in many industries, including financial, insurance, retail, healthcare, legal, electronics, automotive, government and telecommunications. This broad industry knowledge allows for more wide-ranging solutions, encompassing not only our clients' industries, but also those of their customers and suppliers.

Equivus consultants specialize in all aspect of information technology with focus on network infrastructure design, security, Microsoft server applications, Rightfax , disaster recovery and web based technologies.

About the Equivus Communicator

We hope the Equivus Communicator has been of substantial use. If you want to receive future issues or a free onsite evaluation, please contact us via email at info@equivus.com or call 866-378-4887

EQUIVUS

Equivus Inc.
4238b N. Arlington Hts Rd
#361
Arlington Heights, IL 60004
Tel: 866 378 4887
Fax: 815 356 1548
info@equivus.com

Communicator